IN THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently amended) A method of sending a packet from a first IPSec client to a second IPSec client, comprising the steps of:

    receiving at a non-proprietary format tunneling protocol server from the first IPsec client an IPsec packet wrapped in the non-proprietary tunneling format;

    creating a non-proprietary format tunneling protocol tunnel to the second IPsec client through the non-proprietary format tunneling protocol server;

    establishing a security association between the first and second IPSec clients via the non-proprietary format tunneling protocol server; and

    transmitting the packet through the non-proprietary format tunneling protocol tunnel to the second IPSec client whereby the packet remains unaffected by any address translation or firewall traversal that may occur during transmission.

2. (Original) The method according to claim 1 wherein the non-proprietary tunneling protocol comprises a Layer-2 Tunneling Protocol (L2TP) protocol.

3. (Original) The method according to claim 2 wherein the receiving step includes the steps of:

    opening an LT2P tunnel between the first IP client and the server; and communicating an IPsec packet wrapped in an L2TP format to the server.

4. (Original) The method according to claim 2 wherein the receiving step includes the step of routing an IPsec packet wrapped in an L2TP format to the server via a public address.

5. (Currently Amended) The method according to claim 4 wherein the public address is supplied from the server to the first IPsec client.

Page 2

6. (Original) The method according to claim 5 wherein the step of creating a non-proprietary format tunneling protocol tunnel to the second IPsec client includes the step of providing to the second client a public address identifying the server.

7. (Currently amended) A method of sending a packet from a first IPSec client to a second IPSec client comprising the steps of:

    receiving an IPsec packet wrapped in a Layer 2 Tunneling Protocol (L2TP) format packet from the first IPsec client at a L2TP server;

    setting up an L2TP tunnel from the L2TP server to the second IPsec client;

    establishing a security association between the first and second IPSec clients via the L2TP server; and

    transmitting the packet through the L2TP ~~the~~ tunnel to the second IPSec client whereby the packet remains unaffected by any address translation or firewall traversal that may occur during transmission.

8. (Currently amended) The method according to claim 7 wherein the receiving step includes the steps of:

    opening an ~~LT2P~~ L2TP tunnel between the first IP client and the L2TP server; and

    communicating the IPsec packet wrapped in the L2TP format to the server.

9. (Original) The method according to claim 7 wherein the receiving step includes the step of routing the IPsec packet wrapped in the L2TP format to the L2TP server via a public address.

10. (Currently amended) The method according to claim 9 wherein the public address is supplied from the L2TP server to the first IPsec client.

11. (Original) The method according to claim 7 wherein the step of creating the L2TP tunnel to the second IPsec client includes the step of providing to the second client a public address identifying the L2TP server.

Page 3